REMARKS

This Amendment is in response to the Final Action mailed August 13, 2003. The Office Action rejected claims 1-16 under 35 U.S.C. § 103. Applicants have amended claim 1, 11, and 12, cancelled claims 13-16, and added new claims 17-20.

Claims 1-12 and 17-20 remain pending in the application. Reconsideration in light of the amendments and remarks made herein is respectfully requested.

Claim Objections

The Office Action objected to claims 13-16 under 37 CFR 1.75(c) as being of improper depended form for failing to further limit the subject matter of a previous claim. The Office Action also objects to claims 13-16 for their dependency sequence.

Applicants have cancelled claims 13-16.

Rejections Under 35 U.S.C. § 103

The Office Action rejected claims 1-3 and 8-16 under 35 U.S.C. § 103(a) as being unpatentable over Zuk (U.S. Patent No. 5,745,571) in view of Antognini et al. ("Antognini") (U.S. Patent No. 5,649,185).

The Office Action also rejected claims 4-7 under 35 U.S.C. § 103(a) as being unpatentable over Zuk (U.S. Patent No. 5,745,571) in view of Antognini (U.S. Patent No. 5,649,185) and further in view of Vobach (U.S. Patent No. 5,193,115).

Applicants traverse the rejection in its entirety

The Patent Office has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787 (Fed. Cir. 1984).

To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).

"In determining the propriety of the Patent Office case for obviousness in the first instance, it is necessary to ascertain whether or not the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the reference before him to make the proposed substitution, combination, or other modification." *In re Linter*, 458 F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972).

Applicants submit that prima facie obviousness has not been established in this case.

Zuk (Column 5, lines 1-26) describes that the card generates a random number r, encrypts the random number r, and sends the resulting ciphertext to the point-of-sale (POS) terminal. The POS terminal decrypts the ciphertext to obtain the random number r. The POS terminal then generates a key Ki, encrypts the key Ki using the random number r, and sends the resulting ciphertext to the card. The card decrypts the ciphertext using the random number r, to obtain the key Ki. The card uses this key Ki for generating session keys for subsequent communications.

Antognini (Column 9, lines 33-43) describes that the generator 76 provides an image identifier to the client 10.

However, even if Zuk and Antognini could be combined, they fail to teach the authentication system as claimed. Applicants submit that combining Zuk and Antognini does to provide the claimed secure authentication system.

If the combination of Antognini and Zuk is applied to an access device that reads digital information from a storage medium using access information which shows the storage area of the digital information in the storage medium, the procedure is as follows.

(STEP 1) The access device and the storage medium perform challenge-response mutual authentication.

(STEP 2) The access device sends scrambled access information to the storage medium, and the storage medium receives the scrambled access information. (STEPS 1 and 2 may be performed in reverse order.)

(STEP 3) When the mutual authentication has succeeded, the storage medium descrambles the scrambled access information to obtain the access information, reads the digital information specified by the access information, and sends it to the access device.

This being the case, an unauthorized party can gain access to the storage medium by the following attack procedure.

(step 1) The authentication is performed using an authorized access device.

(step 2) After the authentication has succeeded, the unauthorized party replaces the authorized access device with an unauthorized access device. The unauthorized access device scrambles arbitrary access information and sends it to the storage medium.

(step 3) The storage medium treats the unauthorized access device as the authorized access device, and descrambles the scrambled access information sent from the unauthorized access device to obtain the access information. The storage medium then reads digital information specified by the obtained access information, and sends it to the unauthorized access device.

The same process applies to the case of writing digital information into the storage medium. In both cases, an unauthorized party can access to the storage medium by using arbitrary access information. If the unauthorized party conducts a thorough attack by repeating the above procedure, eventually it will succeed in rewriting or reading desired data.

The present invention, on the other hand, does not allow such unauthorized access to occur. For example, Claim 1 is characterized by the following features:

"when authenticating whether the storage medium is authorized, the access device transmits to the storage medium scrambled access information generated by scrambling access information which shows an area, and authenticates whether the storage medium is authorized according to a challenge-response authentication protocol using the scrambled access information, and

when the storage medium and the access device have authenticated each other as authorized devices, the storage medium extracts the access information from the scrambled access information that was used in the authentication protocol, and the access device reads/writes digital information from/into the area shown by the extracted access information."

In the present invention, if an unauthorized party replaces the authorized access device with an unauthorized access device after the mutual authentication has succeeded, then the unauthorized access device scrambles arbitrary access information and sends it to the storage medium.

Even when this occurs, the storage medium extracts the access information from the scrambled access information that was used in the authentication protocol, so that the unauthorized access device cannot deliver the arbitrary access information to the storage medium. In other words, the unauthorized access device cannot use the arbitrary access information. Hence, any attempted access by an unauthorized party ends up being a failure.

Antognini neither discloses nor suggests a construction in which "an access device authenticates a storage medium according to a challenge-response authentication protocol using scrambled access information and the storage medium extracts access information from the scrambled access information that was used in the authentication protocol" as claimed.

Thus, the claimed invention provides a level of authentication security that cannot be attained by Antognini, Zuk, or their combination. The remaining references also fail to teach or suggest the claimed authentication scheme.

Applicants also submit that the remaining independent claims 11, 12, 17, and 19 include the same novel features noted above.

For the reasons discussed above, Applicants submit that the claimed invention is patentable over the cited references.

In conclusion, the invention claimed in Claims 1, 11, 12, 17, and 19 is not taught or suggested by Zuk in view of Antognini, or any of the other cited references. Withdrawal of the §103 rejection of claims 1-12 is respectfully requested.

Conclusion

In view of the amendments and remarks made above, it is respectfully submitted that the pending claims are in condition for allowance, and such action is respectfully solicited. Authorization is hereby given to charge our Deposit Account No. 19-2814 for any charges that may be due. Furthermore, if an extension is required, then Applicants hereby request such an extension.

Respectfully submitted,

SNELL & WILMER L.L.P.

I hereby certify that this document and fee is being deposited on November 12, 2003 with the U.S. Postal Service as first class mail under 37 C.F.R. § 1.8 and is addressed to Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450.

By: James Lee

Signature

Julio M. Loza
Registration Number 47,758
1920 Main Street, Suite 1200
Irvine, California 92614-7230
Telephone: 949/253-4924

Dated: November 12, 2003